# La cryptographie quantique appliquée aux communications ultra-sécurisées

Jacques Boscq

Puteaux, le 29/10/2018

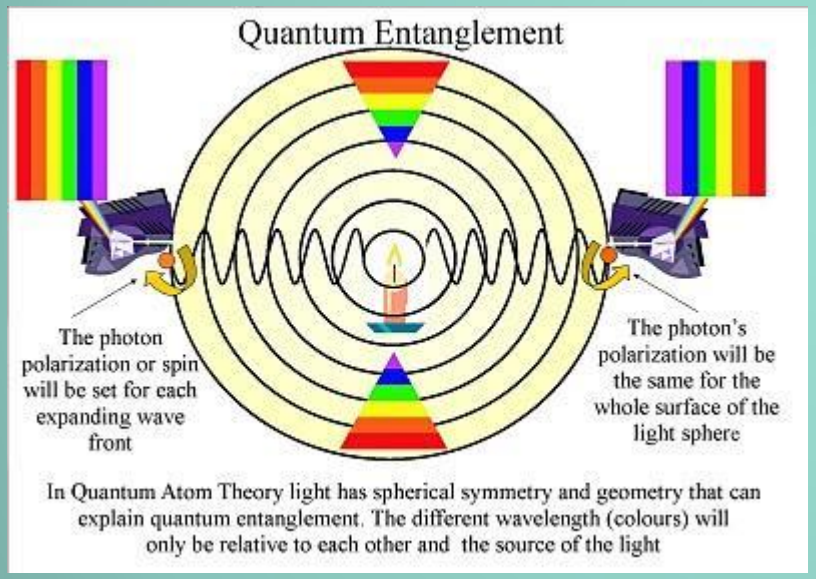
# Programme

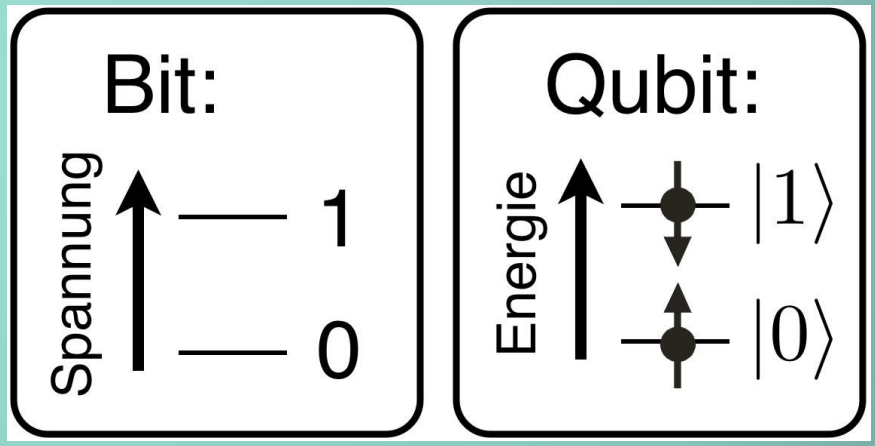
1. Concepts
    a. Science de l’information quantique
    b. Cryptographie quantique
    c. Communication quantique
2. Mécanismes quantiques
    a. Théorème no-go
    b. Réalisme local ou théorie locale des variables cachées
    c. Théorème de Bell
    d. Intrication quantique
3. Applications
    a. Ordinateurs quantiques
    b. Distribution de clé quantique
4. Solutions commerciales existantes
5. Réseaux de distribution de clés quantiques
6. Conclusion

# Concepts

**Science de l'information quantique**

- ◇ **Cryptographie quantique** : utilisation d'effets de la mécanique quantique
- ◇ **Communication quantique** : utilisation de qubits pour le transfert d'états quantiques




**Qu'est-ce qu'un qubit ?**

Système mécanique quantique à deux états (par exemple un photon polarisé).

**Mesurer les états quantiques est perturbant**

Ainsi, détecter les écoutes devient physiquement possible.

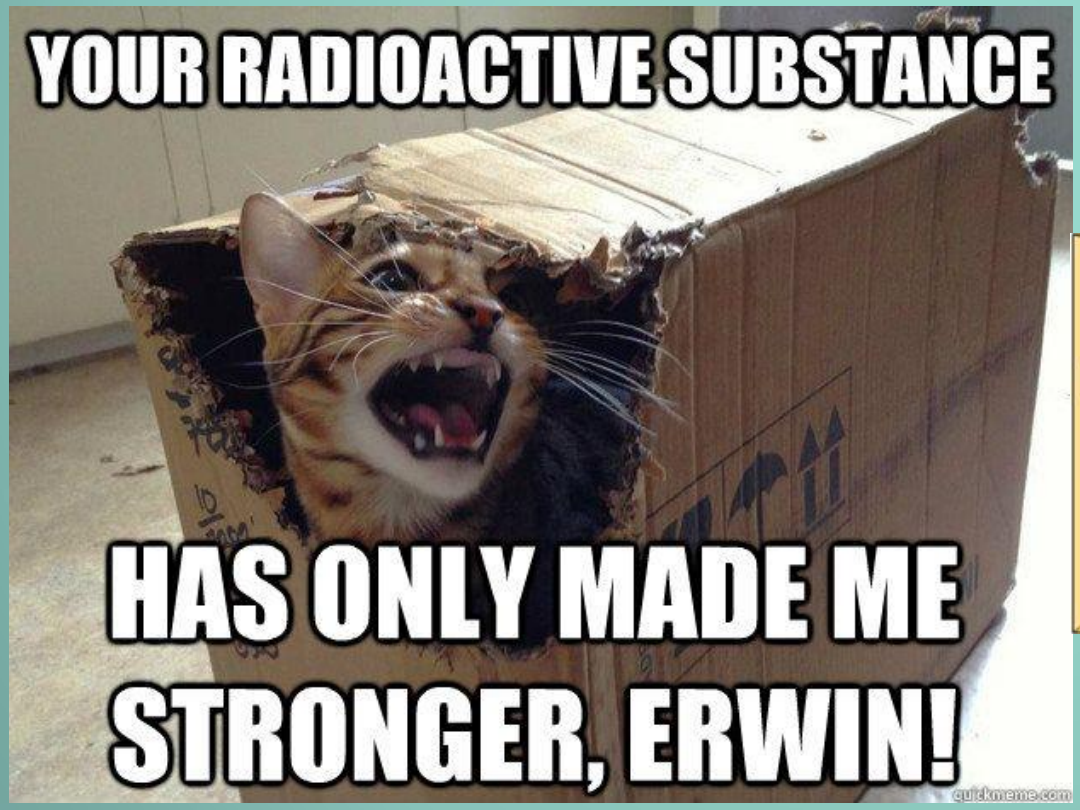
**Intrication quantique**

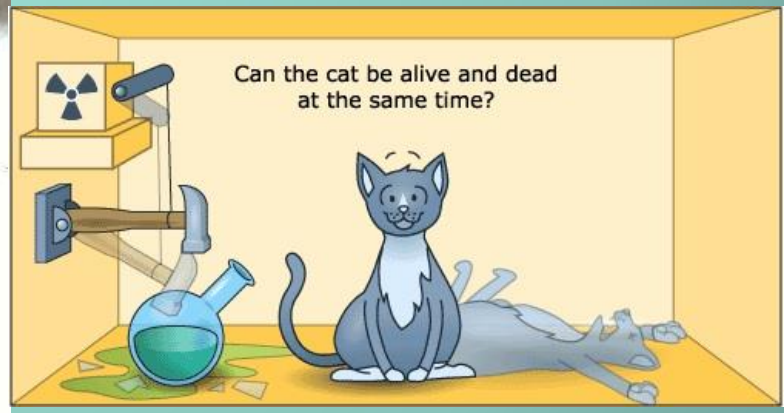
Des (paires de) particules intéragissent avec un état quantique dépendant.

# Concepts


**Chat de Schrödinger**

Expérience de pe**nsée (1935) dans le but d'introduire un paradoxe à l'interprétation de Copenhague.**

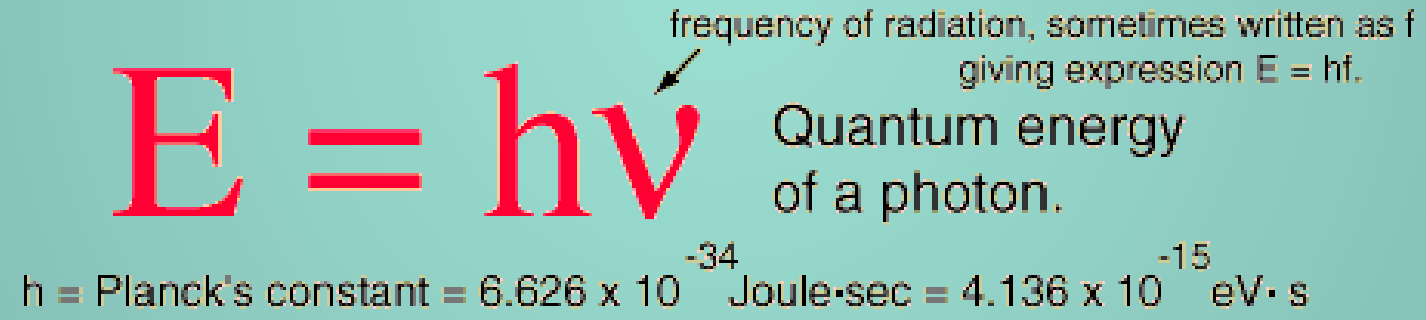


# Concepts

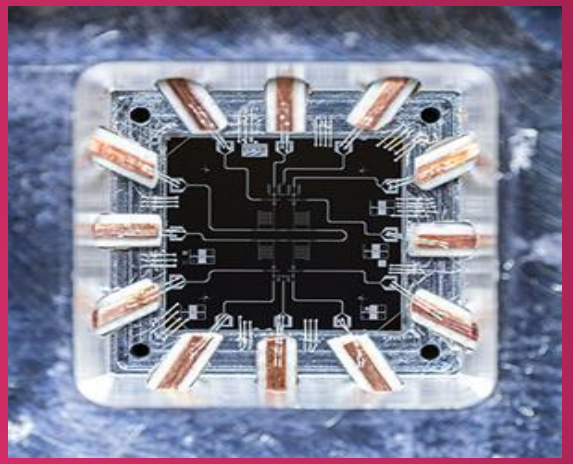
**Mécanismes quantiques**

- **Théorème no-go** : une situation particulière impossible physiquement
- **Réalisme local ou théorie locale des variables cachées** : approche holistique des systèmes physiques
- **Théorème de Bell** : “Aucune théorie physique des variables cachées locales ne peut jamais reproduire toutes les prédictions des mécanismes quantiques”.
- **Interprétation de Copenhague** : la séparation entre l’objet et l’observateur (+ appareils de mesure) est illusoire.

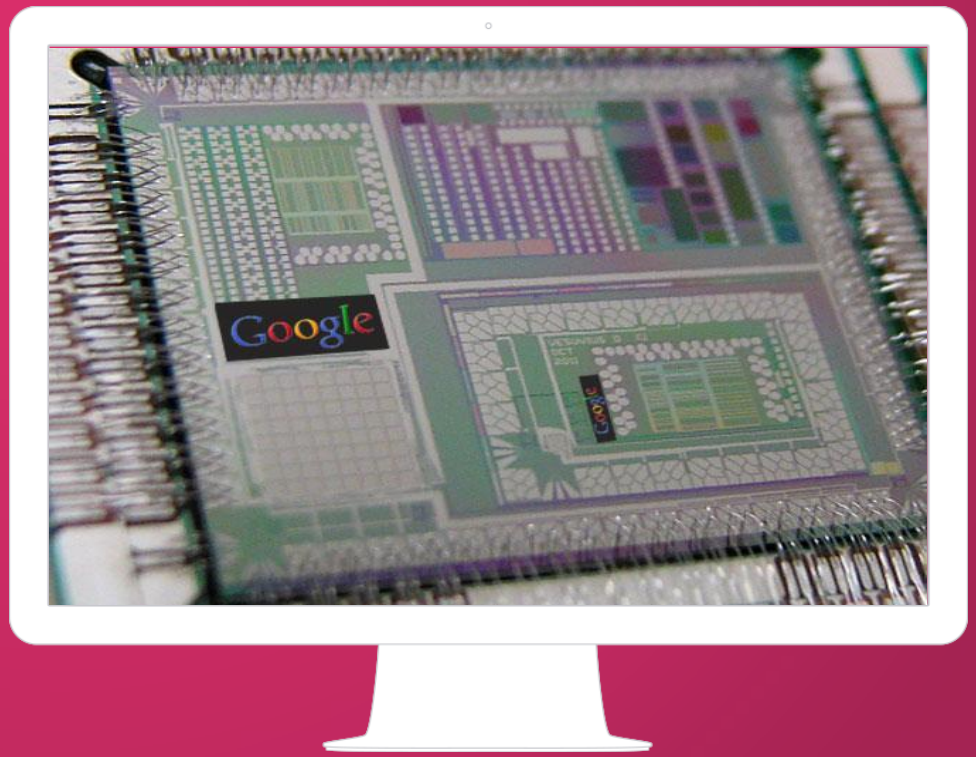



| Constante de Plank | Réalisme local | Théorie locale des variables cachées |
|---|---|---|
| Constante physique représentant le quantum d’action en mécanique quantique. | Le principe de localité + tout objet doit avoir une valeur pré-existante pour toute mesure réalisable. | Théorie hypothétique cherchant à rendre compte des caractéristiques probabilistiques de la mécanique quantique. |

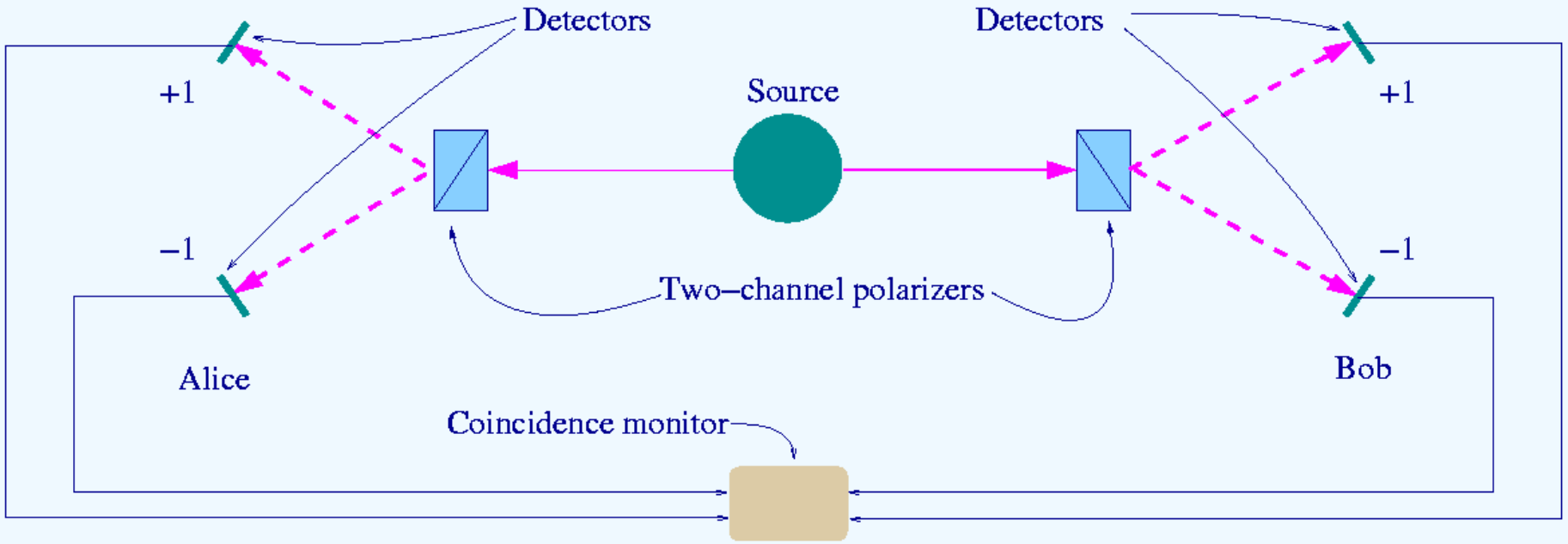
# Ordinateurs Quantiques



En janvier 2017, D-Wave Systems vend le D-Wave 2000Q comportant 2k qu-bits (doublement prévu en 2019), agissant en tant que *recuit simulé* (*quantum annealer*). Dans cette méthode empirique (méta-heuristique) on alterne un cycle de refroidissement lent avec un réchauffage (recuit) ayant pour effet la minimisation de l'énergie du matériau.

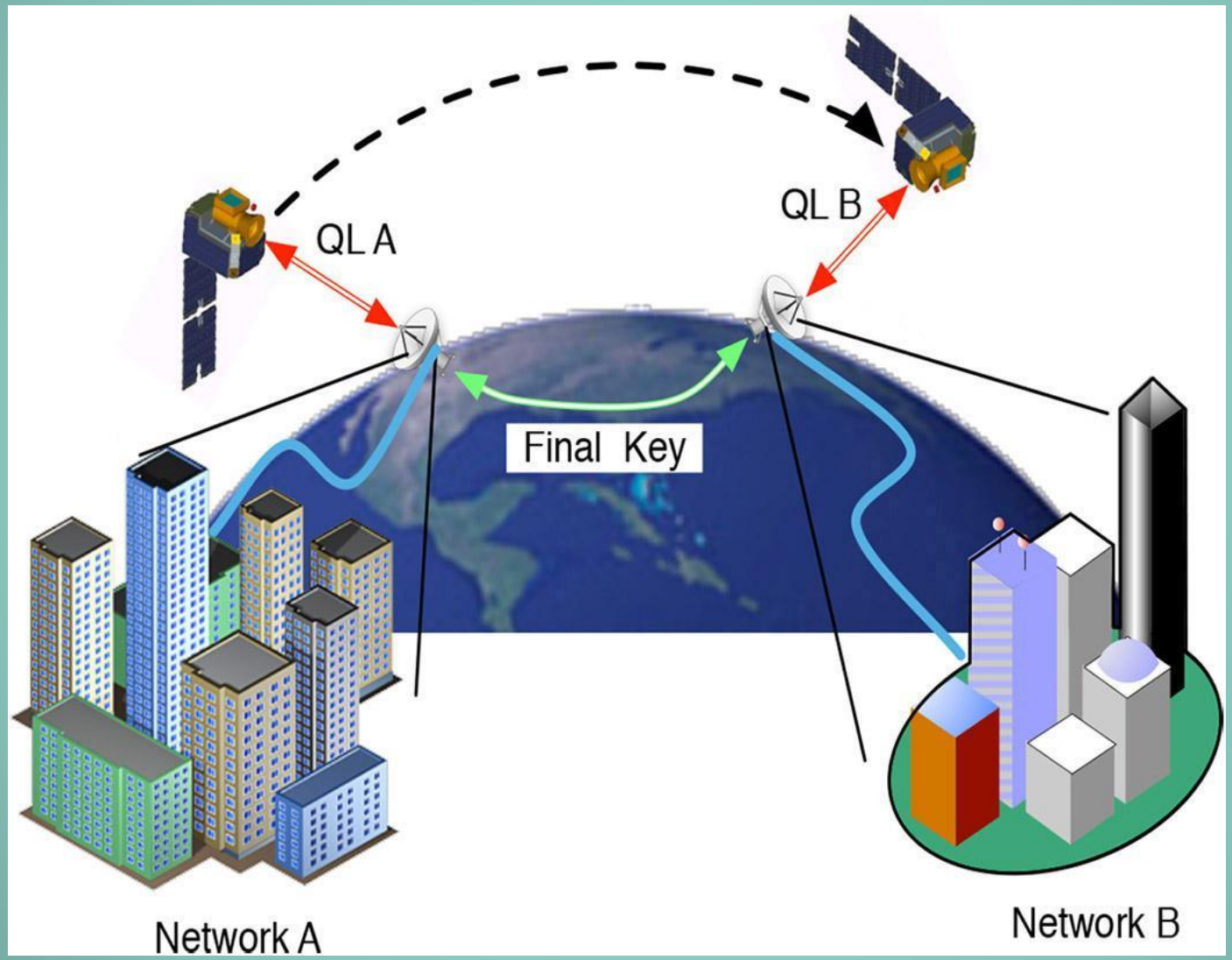


# Expérience pratique testant le théorème de Bell

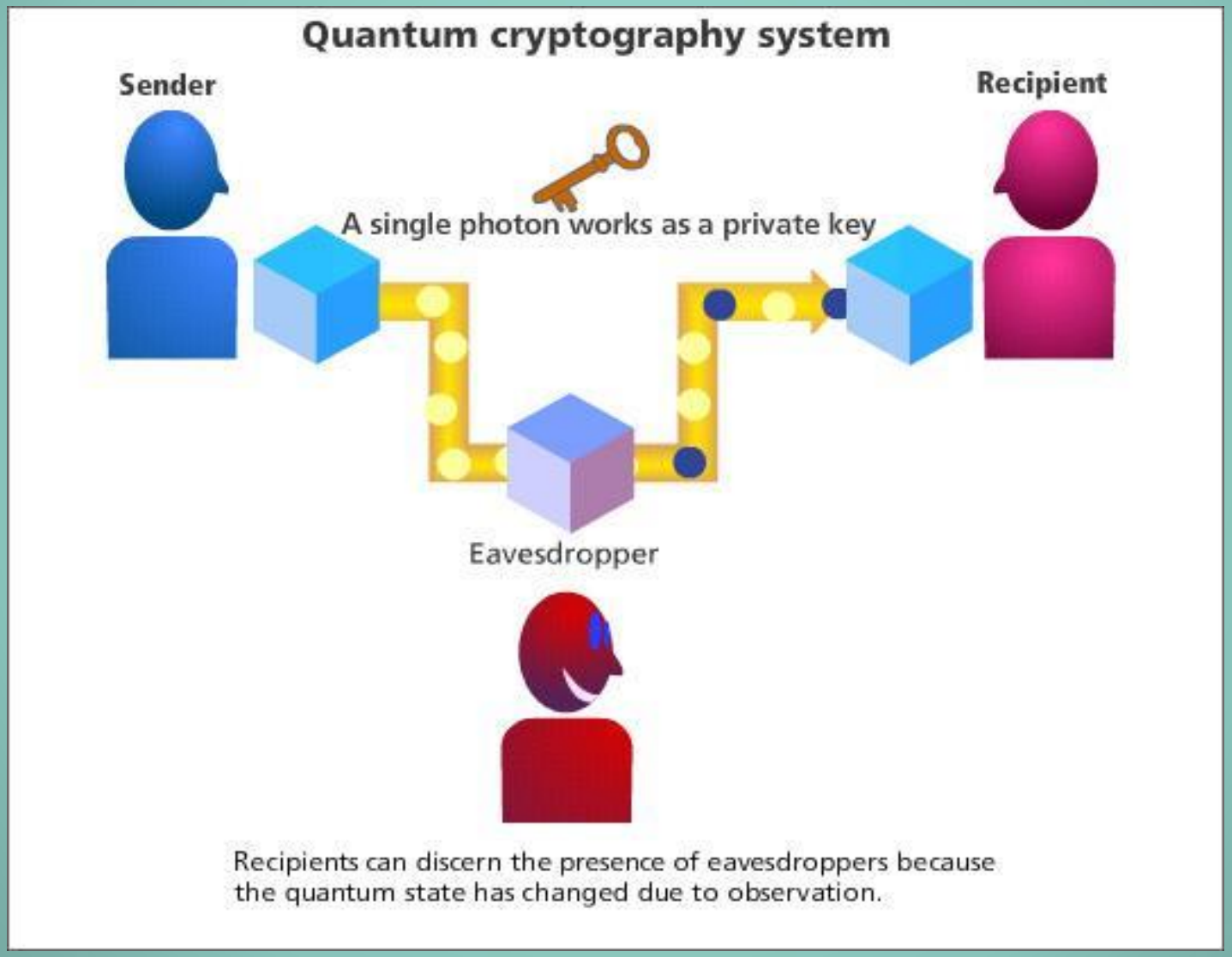



Dérivée du paradoxe d'Einstein-Podolsky-Rosen

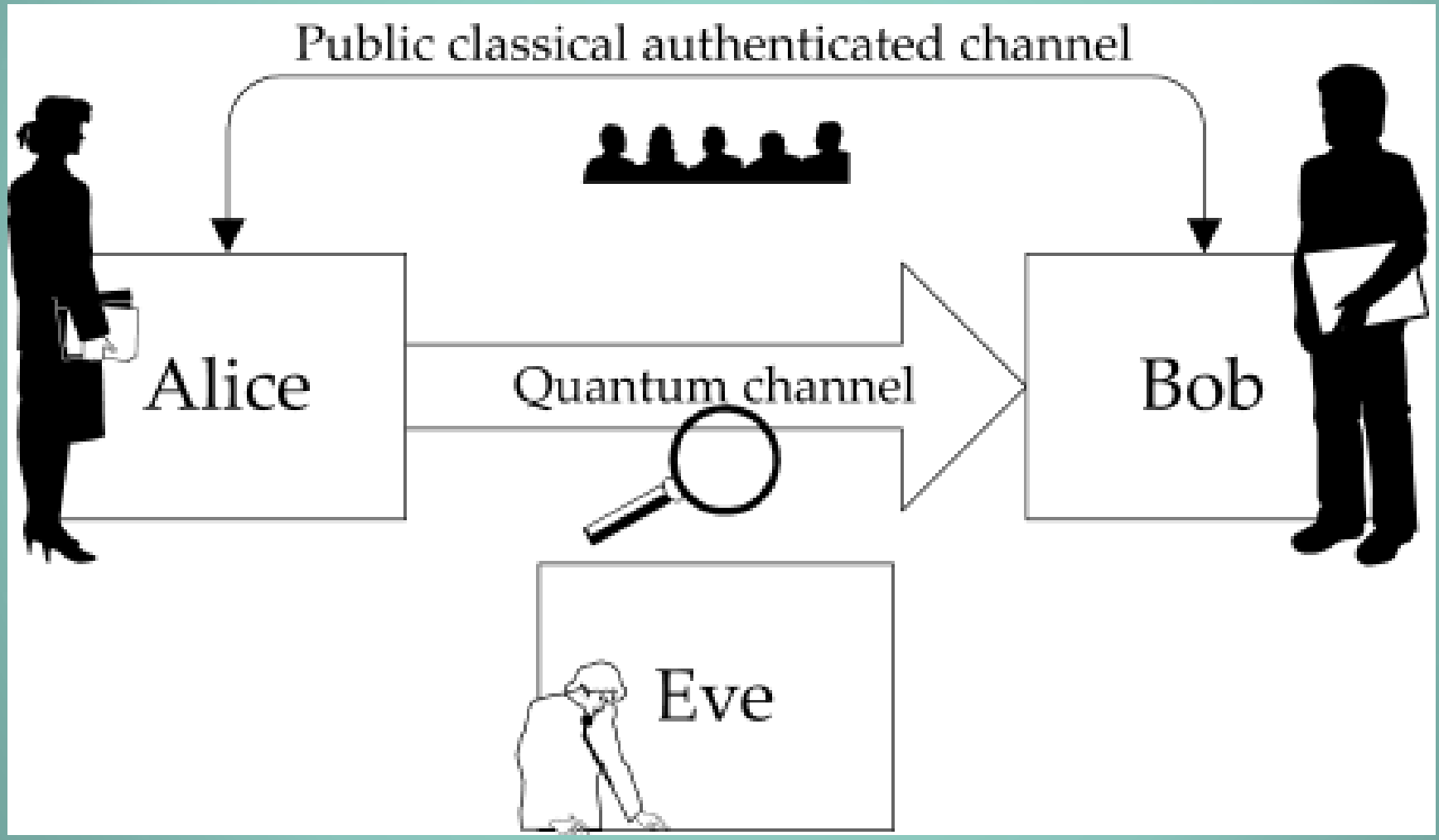
# Communication quantique par satellites



# Schéma de distribution quantique de clés



# Autre schéma de distribution quantique de clés



# Ordinateurs Quantiques

Quelques fournisseurs

quintessence labs
Reinventing Information Security

MITSUBISHI

NTT

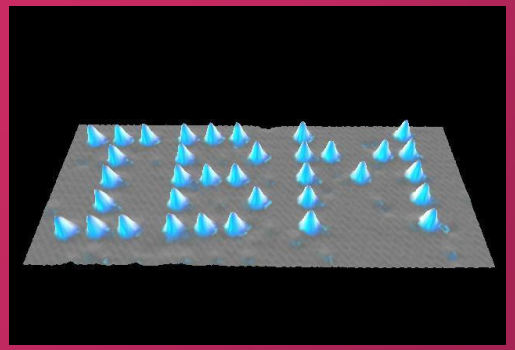
MagiQ™

id Quantique
A Quantum Leap for Cryptography

SEQURENET
A QUANTUM KEY TO NETWORK SECURITY

NEC


hp



# Ordinateurs Quantiques

## QuCube : des Français obtiennent 14 millions d'euros pour construire un CPU quantique de 100 qubits

43

Ce projet est le lauréat de l'appel à propositions de l'ERC (Conseil Européen de la Recherche) Synergy Grant 2018. Il associe trois instituts de recherche français (CEA-Leti, INAC et Institut Néel du CNRS) et obtient un financement de 14 millions d'euros sur six ans pour développer un CPU quantique, explique le CEA.

Les chercheurs espèrent réaliser « *un processeur quantique rassemblant au moins une centaine de bits quantiques (qubit) physiques, et permettant la démonstration d'un premier qubit logique fonctionnel, étape décisive vers un futur ordinateur quantique* ».

« *À l'heure actuelle, ce serait le processeur quantique le plus puissant du monde* » affirme Maud Vinet (CEA-Leti) aux Échos, mais en précisant qu'il peut se passer beaucoup de choses en six ans.

La scientifique explique que « *l'idée de QuCube est de lever les incertitudes sur la possibilité de construire un ordinateur d'un million de qubits* ».

# Réseaux de distribution quantique de clés

- DARPA Quantum network, un réseau de distribution de clés quantiques à 10 noeuds, lancé depuis 2004 au Massachusetts, Etats-Unis
- SECOQC (Secure Communication Based on Quantum Cryptography) interconnecte six villes à Vienne
- SwissQuantum a fonctionné deux ans depuis 2009 (12k heures de fonctionnement)
- Tokyo QKD Network depuis 2010
- Los Alamos National Laboratory depuis 2011




# Bibliographie


Hayford, D. (2014). *The Future of Security: Zeroing In On Un-Hackable Data With Quantum Key Distribution*, from http://www.wired.com/2014/09/quantum-key-distribution/

Hughes, R. (2011). *Satellite-based quantum communications,* from http://adsabs.harvard.edu/abs/2011APS..DMP.K6001H

Jennewein, T. (2014). *Towards Global Quantum Communications using Satellites*, from https://www.youtube.com/watch?v=-cQ5KpoevEQ

Lo, H.K, Curty, M. and Tamaki, K. (2014). *Secure quantum key distribution*, from http://www.nature.com/nphoton/journal/v8/n8/full/nphoton.2014.149.html

Hsu, J. (2014). *Google's First Quantum Computer Will Build on D-Wave's Approach*, from http://spectrum.ieee.org/tech-talk/computing/hardware/googles-first-quantum-computer-will-build-on-dwaves-approach

Preskill, J. (2013). *Quantum Computing and the Entanglement Frontier* from https://www.youtube.com/watch?v=8-IqQnGYB2M

# MERCI

## Questions?

Vous pouvez me joindre à l’adresse :
Jacques@boscq.fr